Location, location, location: the importance of security and privacy of your data in the cloud

Delight your customers with an Agile Cloud Experience

IBM **Cloud**

IBM

Overview

Data - the most valuable business asset for enterprises and their customers, must be protected from unauthorized access. Always available and secure data coupled with insightful data analytics drives business innovation, increases client satisfaction and loyalty – and more importantly, gives you a competitive edge in the marketplace.

Managing data throughout its lifecycle in compliance with business, privacy and security regulatory requirements - must be the top priority in cloud environments. That is why a trusted business partner with deep expertise in security, privacy and cloud deployments is critical. IBM has successfully helped customers migrate to the cloud by using extensive industry-specific products and services backed by more than 2,500 cloud technology patents granted to IBM.

The nature of global cloud computing means that the physical location of data is very relevant and is becoming more significant every day. Business transactions occur across international borders every second. Big data created in one region gets stored, processed, and accessed from other regions across international borders. End users, clients and business partners using your data may be accessing it from all over the globe.

The performance of cloud workloads is proportionate to the user's distance from the data center where your data is housed. This is also true for cloud providers whom are expected to ensure your data moves efficiently with minimal latency around the globe. Knowing this, IBM has invested heavily in building, maintaining and growing an agile global cloud network backbone that transports public and private traffic around the globe to help ensure an exceptional customer experience.

Data location matters

Organizations often migrate business workloads to the cloud so that data is always available and delivered quickly and reliably to customers around the world. The actual location of data is often given little attention due to lack of clarity about concepts such as universal accessibility, guaranteed uptime service level agreements (SLAs) and high-speed network connectivity. Overlooking your data's physical location can lead to slow uploads and downloads, unsatisfactory delays in service, a reduction in productivity, and loss of customers and business. More importantly, where data resides plays an instrumental role in protecting privacy and meeting the regulatory requirements for data protection.

While the cloud delivers infrastructure as a service (IaaS), data stored on the cloud resides on physical storage devices and data in transit traverses physical networks too. Even data used by your cloud applications - data in use - needs to be secured. IBM Cloud provides built-in security solutions designed to protect data throughout its lifecycle.

When looking at the potential performance of global networks, it is customary to use the speed of light in fiber to estimate optimal potential response times as measured in return trip time (RTT).

Cloud workloads require an infrastructure that is agile, secure, responsive and has a local presence on a global scale. IBM understands these business cloud needs and as a response has invested in a global network that offers more than 60 data centers, six multizone regions and six continents. IBM's cloud network keeps application workloads and date secure in data centers that are compliant with regulatory requirements. IBM's data security addresses data at rest, in transit and in use.

IBM Cloud offers IBM Key Protect providing benefits like bring your own keys (BYOK) and IBM Cloud Hyper Protect Crypto Services enabling you to keep your own keys (KYOK) for cloud data encryption.

IBM Key Protect (BYOK)

A multi-tenant Key Management Service (KMS) with key vaulting provided by IBM-controlled FIPS 140-2 Level 3 Hardware Security Modules. With Key Protect, customers bring their keys to the Cloud and manage them, and IBM provides operational assurance that IBM will not access the keys.

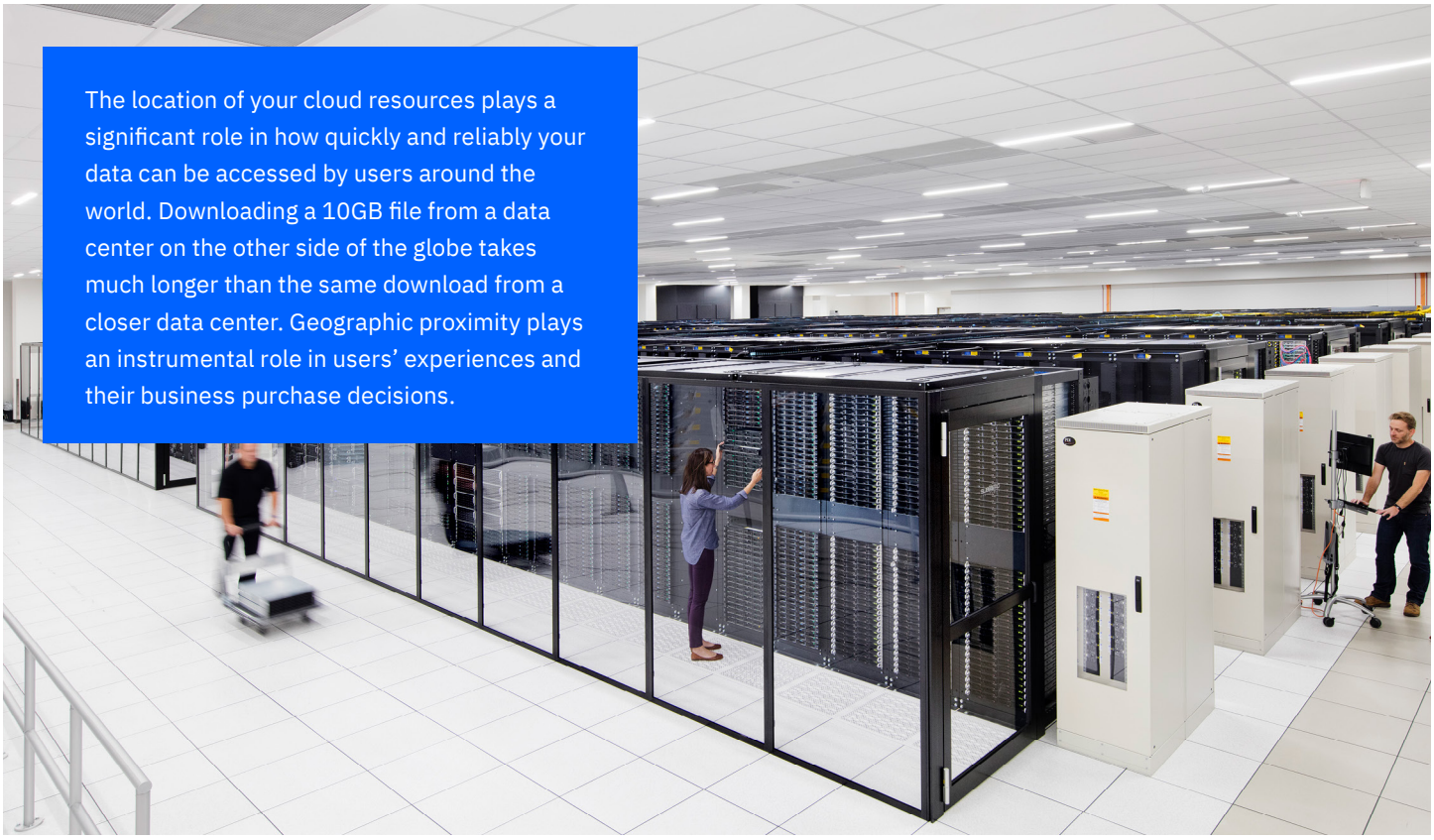
IBM Cloud Hyper Protect Crypto Services (KYOK)

Offers two-in-one (i.e., a KMS with built-in Hardware Security Module (HSM)). The offer is a single-tenant Key Management Service with key vaulting provided by customer-controlled FIPS 140-2 Level 4 HSMs (the highest available certification). **With Hyper Protect Crypto Services, customers keep their keys protected by the HSMs they control and manage; the implementation provides technical assurance that IBM cannot access the keys.**

Customer scenario

The ideal situation for enterprises is to deploy cloud workloads in proximity to their customers for optimal response time. Today's global digital economy means that most enterprises conduct business around the globe and need to ensure that customers, regardless of their location, have pleasant business experiences. For the best experience, the global presence of IBM Cloud affords the opportunity for organizations to deploy their workloads in several locations that are close to their worldwide customer base.

Let's look at a global business that is based in San Jose, CA with customers in Paris, France, and Singapore. The ideal situation for this business is to have workloads deployed as close to these locations – if not directly in these cities – as possible. Alternatively, the business could choose a less optimal solution by deploying workloads in San Jose only; thus giving customers in Paris similar, delayed response times as those in Singapore. With its expansive network, multizone region capabilities and high-speed infrastructure, IBM Cloud is designed to enable businesses to serve their global customers in a secure, fast and timely manner.



The location of your cloud resources plays a significant role in how quickly and reliably your data can be accessed by users around the world. Downloading a 10GB file from a data center on the other side of the globe takes much longer than the same download from a closer data center. Geographic proximity plays an instrumental role in users' experiences and their business purchase decisions.

IBM Cloud global data centers

Protection and delivery of services to customers

IBM Cloud data centers and network points of presence (PoPs) are connected to a global network backbone, which carries public, private, and management traffic to and from servers. This global network boasts more than 2,600Gbps of connectivity between data centers and network PoPs with up to 20 TB of no-cost outbound bandwidth (egress traffic). Additionally, the network PoPs have more than 2,500Gbps of transit and peering connectivity to the Internet. When accessing an IBM Cloud server, the network is designed to bring you onto the IBM global backbone quickly at one of the network PoPs. Clients and end users may experience fewer hops (and a more direct route that IBM Cloud controls). When a user requests data from an IBM Cloud server, that data travels to the nearest network PoP where it is handed off to another provider to carry the data the remaining distance.

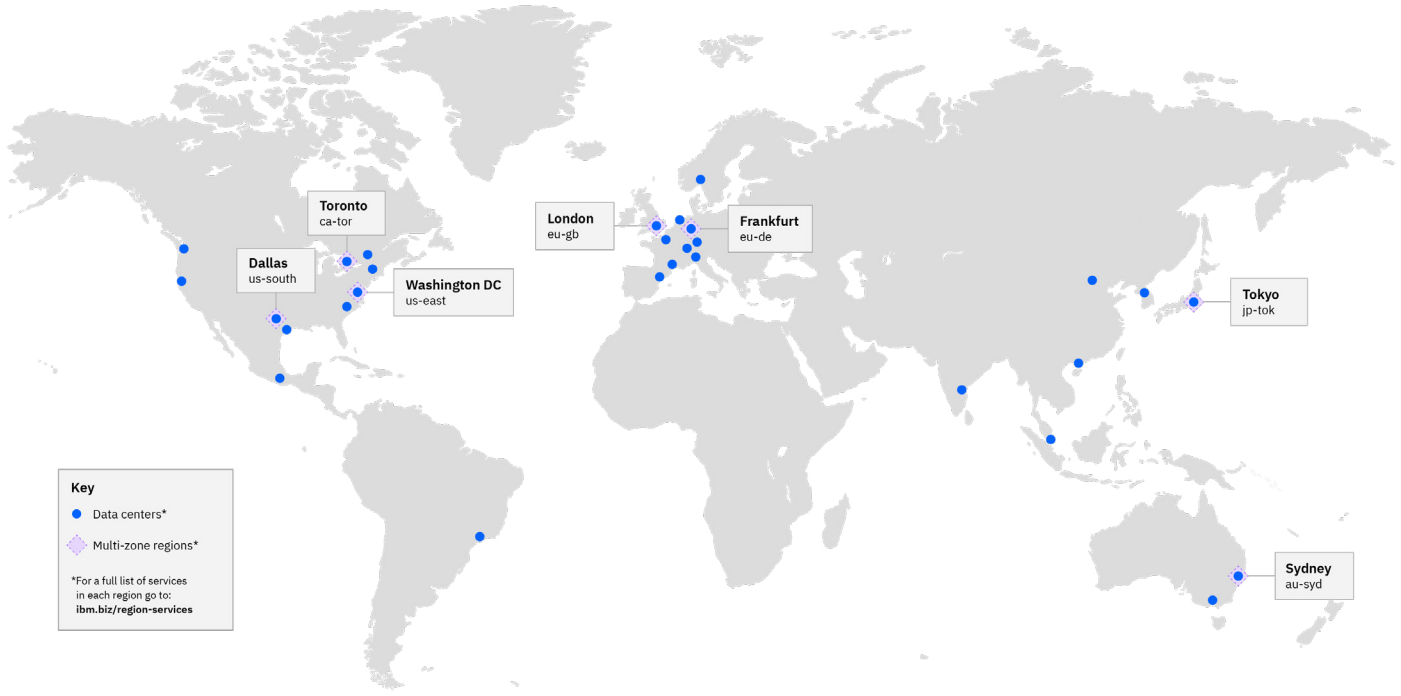


Figure 1: IBM Cloud global data centers and multi-zone regions

Move data securely and quickly

Ensuring your data is secure and protected during a migration and throughout its lifecycle is a critical priority. IBM Cloud uses the same software technology and expertise from on-premises infrastructure making the move to cloud more streamlined and secure. Two examples of this technology are IBM Aspera on Cloud and IBM Cloud VPC.

IBM Aspera on Cloud

When utilizing IBM Aspera on Cloud, enterprises can move files and data sets of any type and size reliably at maximum speed regardless of network conditions. IBM Aspera on Cloud uses patented network-optimized proprietary protocol Fast and Secure Protocol (FASP) to securely move data with security and at speeds that often exceed one hundred times the speed delivered by Transmission Control Protocol (TCP). Data transfers using FASP are encrypted for securing your data at rest and in transit. This solution is designed for quick, reliable and secure movement of large files and data sets between clouds and on-premises resources.

IBM Cloud Virtual Private Cloud (VPC)

Build cloud native 3-tier applications on IBM Cloud Virtual Private Cloud (VPC), which offers a protected space in IBM Cloud with advanced security of a private cloud and the agility and ease of public cloud. This allows you to control virtual networks in logically isolated segments to quickly deploy and manage compute, storage and networking cloud resources. IBM Cloud VPC adds to the security capabilities of the IBM Cloud and creates more secure environments for application workloads and data through the use of security groups and access control lists.

To ensure enterprise workloads and cloud native applications are continuously available, IBM Cloud has multizone regions (MZR) comprised of three availability zones, per MZR, with added fault tolerance that can be leveraged by building workloads using multiple subnets within a single VPC. In addition, IBM Cloud Virtual Server for VPC offers an excellent solution for network-intensive applications, simulations, or in-memory caching with general purpose profiles that provide up to 80Gpbs of network performance.

Multizone regions and availability zones

Deploy workloads in over 60 data centers into 6 regions and 18 availability zones

IBM Cloud is constantly expanding its global footprint to help ensure you're meeting your customers where they are. Our IBM Cloud multizone regions (MZRs) have three or more data centers within six miles of each other. These data centers are located in close proximity to ensure high availability and resiliency. They offer a full and consistent set of services to support your enterprise-class workload needs. MZRs include the full IBM Watson and Cloud stack (IaaS, CaaS, PaaS, cognitive, and data), and are connected to two POPs to help provide maximum POP resiliency. High-speed metro-area interconnects allow applications to have less than 2 millisecond latency in cross zone communications. IBM Cloud Services, such as cloud object storage, containers, API and de-identify data under applicable permissions, are regionally aware and take advantage of this solution easing the burden on the application provider.

IBM Cloud multizone region (MZR)

Availability and resiliency

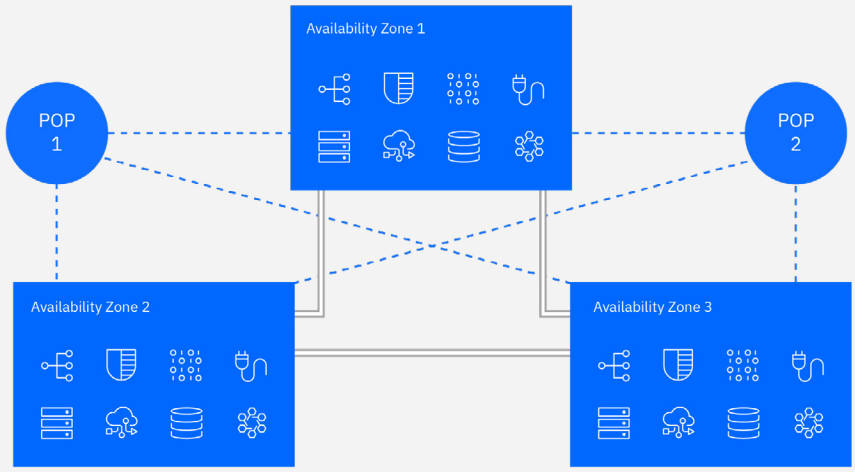
Full system fault tolerance that keeps your business running.

High scalability

Flexible capacity that adapts to changing business production requirements.

Low latency

More responsive applications and faster data movement for better business outcomes.



Our responsibility to you

Data is the most valuable business asset of our time. It's the world's new natural resource, growing exponentially not only in quantity but more importantly, form and value. Every action and interaction, every decision and relationship, every event occurring in any of the world's complex systems, is now expressed as data. This profound shift is compelling enterprises to adopt new technologies and business architectures, based on cloud; and new business processes, skills, and forms of engagement. In the rush to harness potential business value from data, cloud providers mustn't lose sight of basic expectations that individuals, enterprises, and communities rightly have regarding security, trust, privacy, jobs, skills – and, increasingly, the data they own or that is collected from them.

Data ownership and privacy

IBM Cloud believes that the unique insights derived from our clients' data are their competitive advantage, and we do not share them without clients' explicit agreement. We employ security practices to help safeguard data, including the use of encryption, access control methodologies, and proprietary consent management modules, which allow us to restrict access to authorized users.

We advocate for strong and innovative means to enhance privacy and data protection, and we will continue to invest in privacy enhancing technologies. We were an early adopter to the European Union (EU) Data Protection Code of Conduct for Cloud Service Providers for several IBM Cloud services and offering – securing certification under the U.S.-EU Privacy Offerings and the APEC Cross-Border Privacy Rules. IBM was the first cloud provider to deliver hyper data protection and commit to the EU's General Data Protection Regulation (GDPR) compliance. IBM Cloud is GDPR compliant.

Data flows and access

Protecting the privacy of your data, which is fundamental in our data-driven society, is something that IBM Cloud appreciates and is fully committed to. IBM Cloud is making significant investments in our cloud data centers around the globe to give clients the flexibility to decide where to store and process their data. We believe these decisions generally should be driven by client choice rather than government mandate.

Data security and trust

IBM Cloud employs security practices and technologies to help safeguard workloads and data. On the IBM Cloud, data is protected while at rest, in transit and in use. We're poised at the forefront of applying artificial intelligence capabilities to stay steps ahead of emerging digital threats. We do not put 'backdoors' in our products for any government agency, nor do we provide source code or encryption keys to any government agency. You are the only party that would own your encryption keys and not even IBM would have access to those keys. IBM Cloud security builds on IBM heritage of providing proven-in-the-field tested security solutions used by thousands of enterprises worldwide.

Resources

Deploy locally and scale globally.

To learn more about IBM Cloud data centers, visit:
https://www.ibm.com/cloud/data-centers/

Never neglect your network. Learn how to design your cloud to boost traffic and protect your data.

Learn more about IBM Cloud Network:
https://www.ibm.com/cloud/network

The data economy is evolving rapidly.

Read our views on data responsibility:
https://www.ibm.com/blogs/policy/dataresponsibility-at-ibm/

IBM Cloud
New Orchard Road
Armonk, NY 10504
Produced in the United States of America
October 2020